REMARKS

Reconsideration of the pending application is respectfully requested in view of the following observations.

1. In the claims

Claims 1 and 10 have been amended to clarify that the difference in quality is of the user authentication methods. Support for this amendment may be found at least on page 8, lines 14-18 of the Specification.

The claims are now considered to be placed in condition for allowance.

No new matter is introduced via the amendment to the claims.

Entry of the amendment to the claims is kindly requested.

2. Rejection of claims 1-6 and 8-14 under 35 USC 102(e) over US publication 2002/0016913 (*Wheeler*)

Reconsideration of the rejection is respectfully requested in view of the amendment to the claims and the following observations.

Claim 1 recites a method for effecting a secure electronic transaction on a terminal using a portable data carrier. The portable data carrier is arranged to perform different quality user authentication methods. The portable data carrier performs a user authentication using one of the different user authentication methods. The portable data carrier confirms the proof of authentication to the terminal, and the portable data carrier then performs a security-establishing operation within the electronic transaction comprising the steps of the portable data carrier creating authentication quality information about the user authentication method used and attaching the authentication quality information to the result of the security-establishing. The difference in quality of the user authentication methods varies between an inherently relatively lower quality and an inherently relatively higher quality from a security perspective.

Wheeler is directed to a system and method of authenticating a user for entrance into different areas of a building with different levels of security using a single IC card. When gaining entrance to a secure building (3002), the card reader (3004) next to the entrance is initialized (see paragraph [0342]). Once the card reader is initialized, the user (46) enters a PIN using the keypad, and the reader (3004) transmits the PIN to the IC card (95). The IC

card then determines whether the PIN verification data matches the prestored PIN from memory location (76) (see paragraph [0343]).

If the PIN matches, then when the IC card (95) receives the message input command from the card reader (3304) requesting user information, the computer chip (50) on the IC card (95) performs a multi-step process to generate the digital signature (see paragraph [0345]). After the digital signature is generated, the IC card exports the digital signature, user information, and value of the identification marker to the card reader. The card reader is connected to a building security controller (3014), and once the card reader receives the exported information, the information is communicated to the building security controller (3014). The building security controller then uses the exported information to determine whether access should be granted (see paragraph [0346]).

A similar procedure is applied when a retina scan is used instead of a PIN code with the exception that the IC card determines how closely the retina scan matches the stored biometric verification data (see paragraph [0348]). Again, the building security controller uses the IC card generated digital signature, the user information, the value of the identification marker, and the degree to which the retina scan matches the stored biometric verification data to determine whether access should be granted to the room (3102). The building security controller compares the degree of match to a threshold to determine whether access should be granted or denied or if another retina scan is required (see paragraph [0352).

It is submitted that *Wheeler* fails to teach each and every feature of claim 1.

First, *Wheeler* fails to teach that the portable data carrier confirms the proof of authentication to the terminal for all user authentication methods. In *Wheeler*, the building controller determines whether or not access should be granted to the user. The IC card (95) is merely used to generate data to authenticate the user and does not actually perform the final decision of whether or not the user is authenticated for access regardless of the authentication level used. Further, when the retina scan is used the IC card is only used to compare the degree to which the retina scan data matches the biometric verification data (see paragraph [0348]). Thus, *Wheeler* does not teach that the IC card confirms proof of authentication to the building controller for every authentication method.

Second, *Wheeler* does not teach the portable data carrier creates the authentication quality information and that the authentication quality information is about the user

authentication method used. Claim 1 specifies that the difference in quality of the user authentication methods varies between an inherently relatively lower quality and an inherently relatively higher quality from a security perspective. In the instant application, an example of a lower quality authentication method is the use of a PIN check, and an example of a higher quality authentication method is the use of at least one biometric method (see Specification, page 4, line 28 – page 5, line 3). Thus, the authentication quality information indicates the inherent quality of the method used in authenticating the user (see Specification, page 8, lines 14-15) and not the quality of the actual authentication.

Wheeler does not teach the authentication quality information as required by claim 1 since the results of the comparisons performed in the IC card cannot be considered to be authentication quality information. In the case of PIN authentication, the IC card sets the verification status (Rs) to a specific number depending on whether the entered PIN matches the stored PIN. In the case of biometric authentication, the IC card uses the digitized version of the retina scan to determine the degree to which the digitized version matches the stored biometric verification data. The degree of match is set as Rb(016) which corresponds to the percentage match (see paragraph [0348]). In summary, the verification status is a variable which indicates to what degree the received verification data matches the stored verification data. The verification status does not explicitly indicate to the building controller which verification method was used only the degree to which the verification data match which relates to the quality of the actual authentication and not the quality of the authentication method used as required by claim 1.

Moreover, *Wheeler* does not teach that in the security-establishing operation within the electronic transaction, the portable data carrier creates the authentication quality information and that the authentication quality information is about the user authentication method used. During generation of the digital signature in *Wheeler*, the IC card uses the current value of the identification marker, modified user information, and a hash value to generate the digital signature (see paragraph [0345]). None of the steps used by *Wheeler* to generate the digital signature involve creating authentication quality information where the authentication quality information is about the type of user authentication method used as required by claim 1. Therefore, *Wheeler* fails to disclose the creation of authentication quality information about the user authentication method used.

Next, the authentication process performed in *Wheeler* is not performed during a secure electronic transaction. Claim 1 is a method for effecting a secure electronic transaction using a portable data carrier where the portable data carrier performs a security-establishing operation within the electronic transaction. During a transaction, an exchange or transfer of goods, services, or funds occurs. *Wheeler*, however, performs no such electronic transaction. *Wheeler* is purely concerned with authenticating the user for entry into various physical spaces with different levels of security. Further, this authentication process cannot be considered to be an electronic transaction since no transfer of goods, services, or funds occurs during the authentication process. *Wheeler* only communicates data needed to authenticate the user between the IC card and the building security controller.

In contrast, in the instant application, within the electronic transaction, the portable data carrier processes data records which may be related to an electronic banking transaction are supplied from the terminal and returns the data records back to the terminal (see Specification, page 3, lines 10-13). The instant application further discloses that an actual transaction may be the movement of money between two accounts or the initiation of a delivery of goods following an order (see Specification, page 3, lines 14-16).

Lastly, *Wheeler* does not teach that the authentication quality information is attached to the result of the security-establishing operation. Claim 1 recites a separate step after the result of the security-establishing operation is obtained which attaches the authentication quality information about the user authentication method to this result. In *Wheeler*, however, after the digital signature is generated, the IC card transmits the digital signature along with the requested user information, and value of the identification marker to the card reader (3004) (see paragraph [0345]). The value of identification marker is merely the actual quality of the authentication and does not indicate the quality of the authentication method used.

Further, *Wheeler* is silent as to how the digital signature, requested user information, and value of the identification marker are exported to the card reader (3004). Using these three items, the building controller (3014) performs the final authentication (see paragraph [0346]). The building security controller (3014) confirms that the user information matches the name of an authorized employee or employee account number. Then, the building security controller (3014) decrypts the digital signature to determine whether the digital signature contains the unique private key. The last step in the authentication process is the building security controller checking the verification status to determine whether the user of

the IC card is actually the authorized user of the IC card. *Wheeler* does not disclose that any information is attached to the digital signature.

Claim 1, however, requires that the authentication quality information about the user authentication method used be attached to the result of the security-establishing operation. As a result of this attachment, the quality information is firmly joined with the digital signature to form a security message (see Specification, page 8, lines 14-18). Thus, *Wheeler* fails to teach attaching the authentication quality information to the result of the security-establishing operation.

Accordingly, *Wheeler* fails to teach each and every feature of claim 1.

Claim 10 contains similar features to claim 1 and is likewise allowable for the reasons discussed above in claim 1. Moreover, claims 2-6, 8, 9, and 11-14 depend from claim 1 or claim 10 and are likewise allowable in view of their dependency from claim 1 or claim 10 and their individually recited features.

Therefore, withdrawal of the rejection of the claims in view of the prior art is kindly requested.

3. Rejection of claim 7 under 35 USC 103(a) over US publication 2002/0016913 (*Wheeler*) in view of US patent 7,403,765 (*Miyashita*)

Claim 7 depends from claim 1 and is likewise allowable for the reasons discussed above in view of its dependency from claim 1 and its individually recited features. Moreover, *Miyashita* does not cure the deficiencies of *Wheeler*.

Therefore, withdrawal of the rejection of the claims in view of the prior art is kindly requested.

4. Conclusion

As a result of the amendment to the claims, and further in view of the foregoing remarks, it is respectfully submitted that the application is in condition for allowance. Accordingly, it is respectfully requested that every pending claim in the present application be allowed and the application be passed to issue.

If any issues remain that may be resolved by a telephone or facsimile communication with the applicant's attorney, the examiner is invited to contact the undersigned at the numbers shown below.

BACON & THOMAS, PLLC
625 Slaters Lane, Fourth Floor
Alexandria, Virginia 22314-1176
Phone: (703) 683-0500
Facsimile: (703) 683-1080

Date: November 3, 2010

Respectfully submitted,

/Justin J. Cassell/

JUSTIN J. CASSELL
Attorney for Applicant
Registration No. 46,205